UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/608,550	06/30/2003	Ben Smith	0026-0027	7373

44989 7590 12/23/2009

HARRITY & HARRITY, LLP
11350 Random Hills Road
SUITE 600
FAIRFAX, VA 22030

EXAMINER	
NOORISTANY, SULAIMAN	
ART UNIT	PAPER NUMBER
2446	
MAIL DATE	DELIVERY MODE
12/23/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/608,550	SMITH ET AL.	
	Examiner	Art Unit	
	SULAIMAN NOORISTANY	2446	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 September 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-11,15-32 and 34-46* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11 and 15-32, 34-46* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *6/30/2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Detailed Action

This Office Action is response to the application (10/608550) filed on 12/16/2009

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114. including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 7 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 1/18/08 has been entered.

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claims 1-2, 4-11, 16-21, 23-30, 33-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Srinivasan** U.S. Patent App. Publication No. **US 2002/0042738** in view of **Messer** US **U.S. Patent No.** 7020622 further in view of further in view of **Mason** U.S. App. Publication No. **US 2002/0161648.**

Regarding claim 1, Srinivasan teaches wherein, a method performed by a server, the method comprising:

collecting, by one or more processors of the one or more server devices,

information associated with a group of users visiting a web site that include an advertisement link, where he group of users visiting the web site **(example, visitors may be clustered into socioeconomic groups, and only certain groups are sampled when determining an optimal advertisement. In this case, the population may be segmented according to one or more variables, such as income, zip code, profession, previous buying history or the like [0100])**

Identifying, by a processor, non-malicious users visiting the web site from the group of users visiting the web site based on the collected information **(visitors may be identified for sampling based upon prior purchasing history or other accumulated data -- [0100]);**

identifying, by one or more processors of the one or more server devices, a first proportion of a number of non-malicious users visiting the web site to a total number of users visiting the web site **(It is estimated in this example that the website receives 100,000 visitors a day. In this case, the five ads--Ad A, Ad B, Ad C, Ad D and Ad E are input into the system —[0014])**; and

identifying a second proportion of a clicks on the advertising link by identified non-malicious users to a total number of clicks on the advertising link by group of users **(every ad met the minimum threshold of 0.001, and therefore none are dropped. Ad C is determined to be the most effective ad and may now be distributed to every visitor that visits the website -- [0017])**, and

comparing the identified first proportion to the identified second proportion **(Table 1 – "Table 1 illustrates the results of the first iteration of an experiment conducted using the inventive system" [0014-0018])**.

However, with respect to claim 1, Srinivasan is silent in terms of *"an occurrence of spamming on the web site based."*

Messer teaches that it is well known to determine "an occurrence of spamming on the web site based" **(fraud detection processes which detect Javascript on the affiliate's page that automatically triggers and loops the web page linking codes, artificially creating multiple "clicks" on the promotion – col. 3, lines 9-14);**

identifying a second proportion of a clicks on the advertising link by identified non-malicious users to a total number of clicks on the advertising link by group of users **(fraud detection processes which detect Javascript on the affiliate's page that automatically triggers and loops the web page linking codes, artificially creating multiple "clicks" on the promotion – col. 3, lines 9-14)** in order to make the system more efficient and further equipped to deter fraud and other non-productivity activity (col. 4, lines 40-42).

It would have been obvious to one ordinary skill in the art that when the invention was made to modify Srinivasan's invention by adding a system to includes the ability to track select USER activity while on the Web including interactions with Web pages and click-through navigation to select Web sites where purchases can be executed. Notwithstanding these advancements and advantages, commerce on the web can still be improved upon. Recognizing some of the current difficulties in implementing affiliate

programs has led to the innovations presented herein, as taught by Messer (col. 1, lines 40-50).

Mason further teaches wherein determining an occurrence of spamming includes:

identifying a second proportion of a clicks on the advertising link by identified non-malicious users to a total number of clicks on the advertising link by group of users **(if it is found that a soup advertisement is receiving more click-throughs in the late afternoon and ads for a financial services firm are receiving more click-throughs early in the morning, then the placement of those particular ads can be modified in order to maximize the number of click-throughs for the advertisers – [0029])** and

comparing the identified first proportion to the identified second proportion **(the central processor can determine the total number of times that a derivative advertisement is accessed by any online accessing devices or the number of times that such ads are accessed from different online accessing devices. In this manner, the monitoring and auditing integrity is maintained in order to give the advertiser a true representation of the success of the campaign and to discourage potential fraudulent practices wherein a particular derivative advertising link is accessed repeatedly, many times during a short time period from a single computer in order to increase the perceived number of hits or click-throughs -- [0022])**,

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Srinivasan's invention by utilizing a methods for obtaining Internet-type advertisements, modifying those advertisements to fit designated advertising spaces allotted by a plurality of different and unrelated online newspaper websites, and automatically placing those advertisements. Preferred embodiments permit online advertisements to be tracked, audited and/or modified, at any time during an advertising campaign, as taught by Mason.

Regarding claim 2, Srinivasan, Messer and Mason together taught the method as in claim 1 above. Srinivasan further teaches wherein the collecting information includes: tracking activities of the group of users visiting the web site **(visitors may be identified for sampling based upon prior purchasing history or other accumulated data -- [0100]).**

Regarding claim 4, Srinivasan, Messer and Mason together taught the method as in claim 1 above. Messer further teaches wherein the tracking activities includes: determining whether the users in the group of users have JavaScript turned on **(Once the specific information is placed, the Clearinghouse server, via JavaScript, Perl and/or "C" programming, generates the operative link, including all parameters necessary to implement commerce tracking – col. 5, lines 17-20)**.

Regarding claim 5, Srinivasan, Messer and Mason together taught the method as in

claim 1 above. Messer further teaches wherein the tracking activities includes: determining a type of browser used by the users in the group of users **(The first approach tracks USER visits using cookies to determine Web path – col. 2, lines 15-16)**.

Regarding claim 6, Srinivasan, Messer and Mason together taught the method as in claim 1 above. Messer further teaches wherein the tracking activities includes: determining an interval at which each of the users in the group of users visits the web site **(time interval – col. 6, lies 16-17)**.

Regarding claim 7, Srinivasan, Messer and Mason together taught the method as in claim 1 above. Messer further teaches wherein the web site is a search engine **(search engine – col. 5, lines 26-27)**, and wherein the tracking activities includes: determining a type of items for which searches are performed by the users in the group of users **(Transaction Tracking – col. 1, lines 20-36)**.

Regarding claim 8, Srinivasan, Messer and Mason together taught the method as in claim 1 above. Messer further teaches wherein the tracking activities includes: tracking activities of users in the group of users visiting another web site **(The first approach tracks USER visits using cookies to determine Web path – col. 2, lines 15-16)**.

Regarding claim 9, Srinivasan, Messer and Mason together taught the method as in claim 1 above. Messer further teaches wherein each of the users in the group of users is associated with a cookie identifier, and wherein the tracking includes: using the cookie identifiers to track the activities of the users in the group of users **(During the linking process, the USER has an identifier string appended to the HTTP entry, and possibly a "cookie" placed on their system. These act as a marker to permit tracking of the USER by the Clearinghouse, to determine if and when the USER was involved in a purchase – col. 4, lines 5-11)**.

Regarding claim 10, Srinivasan, Messer and Mason together taught the method as in claim 1 above. Messer further teaches wherein each of the users in the group of users is associated with a cookie identifier, and wherein the identifying non-malicious users includes:

identifying non-malicious users based at least in part on an age of the cookie identifiers associated with the users in the group of users **(The first approach tracks USER visits using cookies to determine Web path; alternatively, incentive forms that use a promotional contest to gain voluntary input of data can be applied to collect USER/site data. Once established, closed looped marketing permits targeting of ads to particular Users based on the stored profile – col. 2, lines 15-20)**.

Regarding claim 11, Srinivasan, Messer and Mason together taught the method as in claim 1 above. Srinivasan further teaches wherein each of the users in the group of users is associated with a network address, and wherein the identifying non-malicious users includes:

identifying the non-malicious users based at least in part on the network addresses associated with the users in the group of users **(cookie – [0100])**.

Claim 16 list all the same elements of **claim 1**, but in system rather than method form. Therefore, the supporting rationale of the rejection to **claim 1** applies equally as well to **claim 16**.

Claim 17 list all the same elements of **claim 1**, but in system rather than method form. Therefore, the supporting rationale of the rejection to **claim 1** applies equally as well to **claim 17**.

Claim 18 list all the same elements of **claim 1**, but in system rather than method form. Therefore, the supporting rationale of the rejection to **claim 1** applies equally as well to **claim 18**.

Claim 19 list all the same elements of **claim 1**, but in system rather than method form. Therefore, the supporting rationale of the rejection to **claim 1** applies equally as well to **claim 19**.

Regarding claim 20, Srinivasan, Messer and Mason together taught the method as in claim 19 above. Mason further teaches wherein, determining a total number of users visiting the web site, and wherein the determining whether the item has been click spammed includes:

comparing the determined click rate for the non-malicious users to a click rate for the total number of users visiting the web site **(the central processor can determine the total number of times that a derivative advertisement is accessed by any online accessing devices or the number of times that such ads are accessed from different online accessing devices. In this manner, the monitoring and auditing integrity is maintained in order to give the advertiser a true representation of the success of the campaign and to discourage potential fraudulent practices wherein a particular derivative advertising link is accessed repeatedly, many times during a short time period from a single computer in order to increase the perceived number of hits or click-throughs -- [0022])**, and

Srinivasan further teaches wherein, determining a total number of users visiting the web site **(A manager for the Internet merchant estimates that 100,000 people visit the website -- [0115]);**

determining that the item has been click spammed when the click rate for the total number of users exceeds the determined click rate for the non-malicious users **(the click-through rate, and the effectiveness threshold is 1% -- [0114] "Note: the**

threshold value determines whether the ad has been spammed or not").

Regarding claim 21, Srinivasan, Messer and Mason together taught the method as in claim 19 above. Srinivasan further teaches wherein the identifying includes:

tracking an activity of users visiting the web site (**information derived from user logins, cookies stored on the user's machine and through the user's IP address -- [0048]**), and

Mason further teaches wherein tracking an activity of users visiting the web site and identifying the group of non-malicious users based at least in part on the tracked **(monitoring and auditing integrity is maintained in order to give the advertiser a true representation of the success of the campaign and to discourage potential fraudulent practices wherein a particular derivative advertising link is accessed repeatedly, many times during a short time period from a single computer in order to increase the perceived number of hits or click-throughs -- [0022])**.

Regarding claim 23, Srinivasan, Messer and Mason together taught the method as in claim 19 above. Srinivasan further teaches wherein, taking remedial measures in response to determining that the item has been click spammed **([0039] -- FIG. 4 is a flowchart illustrating the process used to measure Internet advertising effectiveness by the method and system of the present invention).**

Regarding claim 24, Srinivasan, Messer and Mason together taught the method as in claim 19 above. Srinivasan further teaches wherein, the determining a click rate of the item for the group of non-malicious users includes:

estimating a percentage of non-malicious users visiting the web site **(It is estimated in this example that the website receives 100,000 visitors a day -- [0114])**, and setting a percentage of clicks of the item from non-malicious users to approximately equal the estimated percentage **(the minimum effectiveness threshold is 1%-- [0114]).**

Regarding claim 25, Srinivasan, Messer and Mason together taught the method as in claim 19 above. Srinivasan further teaches wherein the determining whether the item has been click spammed includes:

determining whether an actual click rate of the item for the group of non-malicious users differs from the set percentage of clicks of the item **(The statistics typically include, the number of visitors who actually click-through each advertisement – [0084] and also the percentage of visitors to a website that not only click-through the advertisement, but actually buy the advertised product – [0086])**.

Regarding claim 26, Srinivasan, Messer and Mason together taught the method as in claim 19 above. Mason further teaches wherein the determining a click rate of the item includes:

determining different click rates of the item for the group of non-malicious users, the different click rates corresponding to different time periods **(time period –[0022])**.

Regarding claim 27, Srinivasan, Messer and Mason together taught the method as in claim 19 above. Mason further teaches wherein the different time periods include different times of a day or week **(short time period – [0022] "Note: short time period can be any time of a day and or any day of a week)**.

Regarding claim 28, Srinivasan, Messer and Mason together taught the method as in claim 19 above. Mason further teaches wherein, the different time periods include different months of a year **(short time period – [0022] "Note: short time period can be any month of a year).**

Regarding claim 29, Srinivasan, Messer and Mason together taught the method as in claim 13 above. Therefore, Srinivasan, Messer, Srinivasan and Mason also teach a computer-readable medium containing instructions for controlling at least one processor to perform a method for detecting a spamming of an advertisement displayed by a server, as described above. The method comprising:

Srinivasan teaches wherein identifying non-malicious users visiting the server, wherein identifying the non- malicious visitors invluding that the non-malicuois visitors are not spam program **(information derived from user logins, cookies stored on the user's machine and through the user's IP address -- [0049]);**

determining a click rate of the item for the group of non-malicious users (**the click-through rate and the threshold percentage 1% -- [0114])**

determining whether the item has been click spammed based at least in part on the determined click rate for the non-malicious visitors **(the minimum effectiveness threshold is 1% was determined -- [0114], see Page. 7, Table. 1).**

Regarding claim 30, Srinivasan, Messer and Mason together taught the method as in claim 13 above. Therefore, Srinivasan, Messer, Srinivasan and Mason also teach a server comprising:

Mason teaches wherein a memory configured to store at least one advertisement (**memory of computing device -- [0015])**; and

A processor configured to **(a central processor -- [0016)**:

Cause the at least one advertisement **(ad or banner)** to be displayed **(displayed on a computer screen -- [0016])**,

Identify a number non-malicious users accessing the server **(information derived from user logins, cookies stored on the user's machine and through the user's IP address -- [0049])**

compare the number of non-malicious users to a total number of users to obtain a percentage (**the central processor can determine the total number of times that a derivative advertisement is accessed by any online accessing devices or the number of times that such ads are accessed from different online accessing devices. In this manner, the monitoring and auditing integrity is maintained in**

order to give the advertiser a true representation of the success of the campaign and to discourage potential fraudulent practices wherein a particular derivative advertising link is accessed repeatedly, many times during a short time period from a single computer in order to increase the perceived number of hits or click-throughs -- [0022]),

Srinivasan further teaches wherein set a click rate of the at least one item based at least in part on the percentage **(maximize the click-through rate, and the minimum effectiveness threshold is 1% -- [0114])**, and

determine whether the at least one item has been spammed based at least in part on the click rate **(if the measured effectiveness of an advertisement does not meet a minimum threshold, it is deleted from the advertisements -- [0112], TABLE. 1 – [0016]).**

Regarding claim 34, Srinivasan, Messer and Mason together taught the method as in claim 17 above. Mason further teaches wherein the determining whether the advertisement has been click spammed based at least in part on the determined percentage includes:

comparing the determined percentage of the non-malicious users clicking the advertisement to a percentage of non-malicious users clicking the advertisement from a different time period **((the central processor can determine the total number of times that a derivative advertisement is accessed by any online accessing devices or the number of times that such ads are accessed from different online**

accessing devices. In this manner, the monitoring and auditing integrity is maintained in order to give the advertiser a true representation of the success of the campaign and to discourage potential fraudulent practices wherein a particular derivative advertising link is accessed repeatedly, many times during a short time period from a single computer in order to increase the perceived number of hits or click-throughs -- [0022]).

Regarding claim 35, Srinivasan, Messer and Mason together taught the method as in claim 17 above. Mason further teaches where the determining whether the advertisement has been click spammed includes:

estimating a percentage of non-malicious users clicking the advertisement to be approximately a percentage of non-malicious users accessing the server **(if it is found that a soup advertisement is receiving more click-throughs in the late afternoon and ads for a financial services firm are receiving more click-throughs early in the morning, then the placement of those particular ads can be modified in order to maximize the number of click-throughs for the advertisers – [0029])**, and

Srinivasan further teaches determining that the advertisement has been clicked spammed when the determined percentage of non-malicious users clicking the advertisement is lower than the estimated percentage of non-malicious users clicking the advertisement **(the minimum effectiveness threshold is 1% --TABLE. 1, illustrates the results of the first iteration of an experiment conducted using the**

inventive system – [0016]).

Regarding claim 36, Srinivasan, Messer and Mason together taught the method as in claim 18 above, mason further teaches wherein when determining whether the at least one advertisement has been click spammed, the processor is configured to: compare the determined percentage of the non-malicious users clicking the at least one advertisement to a percentage of non-malicious users clicking the at least one advertisement from a different time period **(if the derivative advertisement links from one original ad are receiving 20% more click-throughs than the derivative advertisement links created from a second original ad, then some or all of the placements of the second original ad can be automatically replaced by the more successful ad -- [0029]).**

Regarding claim 37, Srinivasan, Messer and Mason together taught the method as in claim 18 above, Srinivasan further teaches wherein when determining whether the at least one advertisement has been click spammed, the processor is configured to:

estimate a percentage of non-malicious users clicking the at least one advertisement to be approximately a percentage of non-malicious users visiting the server (**percentage of visitors to a website – [0086])**, and

determining that the at least one advertisement has been clicked spammed when the determined percentage of non-malicious users clicking the at least one advertisement is lower than the estimated percentage of non-malicious users clicking

the at least one advertisement **([0039] -- FIG. 4 is a flowchart illustrating the process used to measure Internet advertising effectiveness by the method and system of the present invention).**

Regarding claim 38, Srinivasan, Messer and Mason together taught the method as in claim 19 above, Mason further teaches wherein where the method further comprises:

determining a total number of visitors to the server, and

where the determining whether the advertisement has been spammed includes: (**the central processor can determine the total number of times that a derivative advertisement is accessed by any online accessing devices or the number of times that such ads are accessed from different online accessing devices. In this manner, the monitoring and auditing integrity is maintained in order to give the advertiser a true representation of the success of the campaign and to discourage potential fraudulent practices wherein a particular derivative advertising link is accessed repeatedly, many times during a short time period from a single computer in order to increase the perceived number of hits or click-throughs -- [0022])**, and

Srinivasan further teaches wherein, determining a total number of users visiting the web site **(A manager for the Internet merchant estimates that 100,000 people visit the website -- [0115]);** determining that the item has been click spammed when the click rate for the total number of users exceeds the determined click rate for the non-malicious users **(the click-through rate, and the effectiveness threshold is 1% --**

[0114] "Note: the threshold value determines whether the ad has been spammed or not").

Claims 3, 15, 22, 31-32 39-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Srinivasan** U.S. Patent App. Publication No. **US 2002/0042738** in view of **Messer** US U.S. Patent No**. 7020622** further in view of **Mason** U.S. App. Publication No. **US 2022/0161648** further in view of **Ishikawa** Patent App. Publication No **US US. 2001/0037314.**

Regarding claims 31, Srinivasan, Messer and Mason together taught the method as in claim 1 above. Therefore, Srinivasan, Messer and Mason further teach a method of claim 31.

However, Srinivasan, Messer and Mason are silent in terms "*loading image*".

Ishikawa teaches wherein "whether the user *loads images"* **(Advertising (graphic) link is loaded onto a user's computer – [0015]).**

Further it would have been obvious to one ordinary skilled in the art in the time the invention was made to combine the teaching of Ishikawa for loading images onto the user's devices, which will provide a generated confirmation code.

Motivation would be to provide a true recognition of the users devices as suggested by Ishikawa for comparing the users information to aspects of the confirmation code, namely, the user identification at the time the advertisement link is loaded onto the user's computer.

Claims 3, 22, 32, 39-40, have the similar limitation as of claim 31; therefore, it's rejected under the same rationale as in claim 31.

Regarding claim 15, Ishikawa further teaches providing a refund in response to determining that the at least one advertisement has been spammed **(Once the information is recorded in the advertiser's log, the entry is further passed to an accounting management system, which tracks the amount of *remuneration* owed to each advertiser, this procedure take place while the click is not spam [0052])**.

Regarding claim 41, Srinivasan, Messer and Mason and Ishikawa together taught the method as in claim 31 above. Srinivasan further teaches wherein where the at least one item includes an advertisement **(a product advertised on the web page – col. 7, lines 60-61).**

Regarding claim 42, Srinivasan, Messer and Mason and Ishikawa together taught the method as in claim 31 above. Srinivasan further teaches wherein:

determining a quantity of the identified non-malicious users that clicks an advertisement associated with the web site **(A manager for the Internet merchant estimates that 100,000 people visit the website -- [0115]);** and

determining whether the advertisement has been spammed based on the determined quantity of the identified non-malicious users that clicks the advertisement

(the click-through rate, and the effectiveness threshold is 1% -- [0114] "Note: the threshold value determines whether the ad has been spammed or not").

Mason further teaches "determined click rate for the non-malicious users to a click rate for the total number of users visiting the web site" **(the central processor can determine the total number of times that a derivative advertisement is accessed by any online accessing devices or the number of times that such ads are accessed from different online accessing devices. In this manner, the monitoring and auditing integrity is maintained in order to give the advertiser a true representation of the success of the campaign and to discourage potential fraudulent practices wherein a particular derivative advertising link is accessed repeatedly, many times during a short time period from a single computer in order to increase the perceived number of hits or click-throughs -- [0022])**

Regarding claim 43, Srinivasan, Messer and Mason and Ishikawa together taught the method as in claim 31 above. Messer further teaches wherein determining that spamming occurs on the web site based on a behavior of the non-malicious users visiting the web site **(fraud detection processes which detect Javascript on the affiliate's page that automatically triggers and loops the web page linking codes, artificially creating multiple "clicks" on the promotion – col. 3, lines 9-14)**.

Regarding claim 44, Srinivasan, Messer and Mason and Ishikawa together taught the method as in claim 31 above. Srinivasan further teaches wherein the determining the

occurrence of spamming on the web site further includes: determining, based on the comparing, that the identified first proportion is greater than the identified second proportion **(Table 1, threshold – [0016])**.

Regarding claim 43, Srinivasan, Messer and Mason and Ishikawa together taught the method as in claim 31 above. Srinivasan further teaches wherein the determining that the occurrence of spamming on the web site further includes: determining, based on the comparing, that the identified first proportion is greater than the identified second proportion plus a predefined threshold **(Table 1, threshold – [0016])**.

Regarding claim 43, Srinivasan, Messer and Mason and Ishikawa together taught the method as in claim 31 above. Srinivasan further teaches wherein the means for identifying malicious visitors comprise means for identifying spam programs **(Table 1, threshold – [0016])**.

Response to Amendment

Applicant's arguments with respect to claim(s) 1-11, 15-32, 34-46 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sulaiman Nooristany whose telephone number is (571) 270-1929. The examiner can non-maliciously be reached on M-F from 9 to 5. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeff Pwu, can be reached on (571) 272-6798. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Sulaiman Nooristany 12/16/2009

/Jeffrey Pwu/

Supervisory Patent Examiner, Art Unit 2446